JAMES R. LANGEVIN
2D DISTRICT, RHODE ISLAND

COMMITTEE ON HOMELAND SECURITY
EMERGING THREATS, CYBERSECURITY, AND
SCIENCE AND TECHNOLOGY
CHAIRMAN

BORDER, MARITIME, AND
GLOBAL COUNTERTERRORISM

INTELLIGENCE, INFORMATION SHARING, AND
TERRORISM RISK ASSESSMENT

HOUSE PERMANENT SELECT
COMMITTEE ON INTELLIGENCE
TERRORISM, HUMAN INTELLIGENCE,
ANALYSIS AND COUNTERINTELLIGENCE

TECHNICAL AND TACTICAL INTELLIGENCE

Congress of the United States
House of Representatives
Washington, DC 20515–3902

WASHINGTON OFFICE:
109 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
TELEPHONE: (202) 225–2735
FAX: (202) 225–5976

DISTRICT OFFICE:
THE SUMMIT SOUTH
300 CENTERVILLE ROAD, SUITE 200
WARWICK, RI 02886
TELEPHONE: (401) 732–9400
FAX: (401) 737–2982

james.langevin@mail.house.gov
www.house.gov/langevin

The Honorable James R. Langevin
Statement on the Implications of Cyber Vulnerabilities on the Resiliency and Security of the Electric Grid”
May 21, 2008

Good afternoon. I'd like to thank our witnesses for testifying today. Over the last year, this Subcommittee has spent a lot of time and energy on improving federal network security. Today's issue – the security of our critical infrastructure networks – is one that demands equal attention.

The effective functioning of our critical infrastructure – from dams and water systems, to factories and the electric grid – is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. This connectivity places these infrastructures at increased risk of intentional or unintentional control system failures, which can have a significant and potentially devastating impact on the economy, public health, and national security of the United States.

There can be no doubt that America's critical infrastructure networks are under constant threat. Pervasive vulnerabilities in hardware and software, and the connectivity of these machines to the Internet make our multilayered lines of defense – anti-virus, firewall, and intrusion detection – relatively ineffective in addressing the problem. To compound matters, many organizations prefer to focus on the deployment of new technology without regard for the security or integrity of their systems or information. This often means that information security officers are simultaneously facing increased responsibilities and shrinking budgets.

These are overwhelming challenges without clear solutions. The federal government and the private sector must act with a sense of urgency to address these issues, and yet, as I read today's testimony, I still do not get the sense that we are addressing cybersecurity with the seriousness it deserves.

Today's hearing will focus on two primary issues. First, we will receive an update from the Federal Energy Regulatory Commission (FERC) and the North American Electric Reliability Corporation (NERC) about electric industry efforts to mitigate a cyber vulnerability known as Aurora. I think we could search far and wide and not find a more disorganized, ineffective response to an issue of national security. Everything about the way this vulnerability was handled – from press leaks, to DHS's failure to provide more technical details to support the results of its test, to NERC's dismissive attitude, to the industry's half-hearted approach towards mitigation – leaves me with little confidence that we are ready or willing to deal with the cybersecurity threat.

As time passes, I grow particularly concerned by NERC, the self-regulating organization responsible for ensuring the reliability of the bulk power system. Not only did they propose cybersecurity standards that – according to the GAO and NIST – are inadequate for protecting critical national infrastructure, but throughout the Committee's investigation they continued to provide misleading statements about their oversight of industry efforts to mitigate the Aurora vulnerability. If NERC doesn't start getting serious about national security, it may be time to find a new electric reliability organization. NERC can begin demonstrating its commitment by incorporating more of the NIST security controls in the next iteration of its reliability standards.

I am thankful that Chairman Kelliher and his staff at FERC are taking cybersecurity seriously. In earlier correspondence, Chairman Thompson and I voiced our concern that the Commission not only lacked authority to regulate potentially vulnerable cybersecurity assets that are not covered in the NERC standards, but also the authority to issue orders to owners and operators in the event of an imminent exploitation of an asset on the grid. The Chairman and I fully support FERC's request for additional legal authorities to adequately protect the bulk power system, and we look forward to working with you and the appropriate committees in the future.

Our second issue of discussion today involves a GAO investigation that this Committee commissioned last year. We asked GAO to provide insight into the cybersecurity controls of the nation's largest public power company, the Tennessee Valley Authority (TVA). The TVA's service area covers 80,000 square miles in the southeastern United States, with a total population of about 8.7 million people. Unfortunately, GAO found that TVA's security posture was seriously lacking. According to the report, TVA has not fully implemented appropriate security practices to secure the control systems and networks used to operate its critical infrastructures. Until TVA addresses these weaknesses, it risks a disruption of its operations as a result of a cyber incident, which could impact its customers.

I am pleased to hear that TVA has taken significant steps towards implementing higher levels of security. But these problems are not unique to TVA. I believe they are typical of security practices across the industry. And, given what we've seen with the Aurora mitigation, I have little confidence that the industry is taking the appropriate actions.

In closing, I'd like to challenge each of you here, and everyone in the industry. Prove to our Committee that you are serious about cybersecurity. Show us you're willing to adopt better standards because it will make the entire grid more secure. Leverage the critical infrastructure community to push control system vendors to build more secure products. And commit the manpower and the money to mitigating your vulnerabilities.

We will continue our oversight in this area. At the next Subcommittee hearing, I look forward to talking about all the progress the industry has made in meeting our challenges.